

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA**

CASE NO. 25-cv-60803-WPD

K.MIZRA LLC,

Plaintiff,

v.

CITRIX SYSTEMS, INC., and
CLOUD SOFTWARE GROUP, INC.,

Defendants.

_____ /

**PLAINTIFF K.MIZRA LLC'S BRIEF IN OPPOSITION
TO DEFENDANTS' MOTION TO DISMISS (ECF NO. 19)**

TABLE OF CONTENTS

TABLE OF AUTHORITIES	ii
I. INTRODUCTION	1
II. APPLICABLE LEGAL STANDARDS	1
III. ARGUMENT	2
A. A Federal Court Has Already Found These Claims Patent Eligible.....	2
B. The '705 Patent Claims Are Not Directed To An Abstract Idea (<i>Alice</i> -Step 1)	3
1. Citrix Fails to Establish that the Claims are directed to an Abstract Idea	3
2. Citrix Fails to Establish That the Actual Claim Language Meets its Proposed Abstract Idea Definition	7
3. The '705 Patent Claims are Directed to a Technological Solution to a Technological Problem.....	8
4. Citrix's Relied-Upon Access Control Cases Demonstrate Non-Abstraction.....	12
C. The Claims Include An Inventive Concept (<i>Alice</i> -Step 2)	13
D. Subject Matter Eligibility Should Not Be Resolved On A Motion To Dismiss	18
E. Claim 19 Is Not Representative Of All Claims	19
IV. CONCLUSION.....	20

TABLE OF AUTHORITIES

Cases

<i>Aatrix Software, Inc. v. Green Shades Software, Inc.</i> , 882 F.3d 1121 (Fed. Cir. 2018).....	14, 20
<i>Aatrix Software, Inc. v. Green Shades Software, Inc.</i> , 890 F.3d 1354 (Fed. Cir. 2018).....	18
<i>Alice Corp. Pty. Ltd. v. CLS Bank Int'l</i> , 573 U.S. 208 (2014).....	1, 13
<i>Amdocs (Isr.) Ltd. v. Openet Telecom, Inc.</i> , 841 F.3d 1288 (Fed. Cir. 2016).....	14, 15, 19
<i>Ancora Techs. v. HTC Am., Inc.</i> , 908 F.3d 1343 (Fed. Cir. 2018).....	passim
<i>Bancorp Servs., L.L.C. v. Sun Life Assur. Co. of Can.</i> , 687 F.3d 1266 (Fed. Cir. 2012).....	18
<i>BASCOM Global Internet Servs. v. AT&T Mobility LLC</i> , 827 F.3d 1341 (Fed. Cir. 2016).....	14, 15
<i>Berkheimer v. HP Inc.</i> , 881 F.3d 1360 (Fed. Cir. 2018).....	17
<i>Broadband iTV, Inc. v. Amazon.com, Inc.</i> , 113 F.4th 1359 (Fed. Cir. 2014)	2, 13
<i>Cellspin Soft, Inc. v. Fitbit Inc.</i> , 927 F.3d 1306 (Fed. Cir. 2019).....	18
<i>Chamberlain Yacht Sales, Inc. v. Phx. Glob. Equity Partners Ltd.</i> , No. 24-60953-CIV-DIMITROULEAS, 2025 U.S. Dist. LEXIS 80562 (S.D. Fla. Apr. 11, 2025)	16
<i>Contour IP Holding LLC v. GoPro, Inc.</i> , 113 F.4th 1373 (Fed. Cir. 2024)	7
<i>Cosmokey Sols. GmbH & Co. AG v. Duo Sec. LLC</i> , 15 F.4th 1091 (Fed. Cir. 2021)	15
<i>Data Engine Techs. Ltd. v. Google LLC</i> , 906 F.3d 999 (Fed. Cir. 2018).....	4
<i>DDR Holdings, LLC v. Hotels.com, L.P.</i> , 773 F.3d 1245 (Fed. Cir. 2014).....	4, 5, 14
<i>DeCurtis LLC v. Carnival Corp.</i> , No. 20-22945-Civ-SCOLA/TORRES, 2021 U.S. Dist. LEXIS 3163 (S.D. Fla. Jan. 6, 2021)	18
<i>Dist. Media Techs., Inc. v. Hulu, LLC</i> , No. 4:16cv245-MW/CAS, 2017 U.S. Dist. LEXIS 179660 (N.D. Fla. July 3, 2017)	13
<i>Ericsson, Inc. v. TCL Commc'n Tech Holdings Ltd.</i> , 955 F.3d 1317 (Fed. Cir. 2020).....	6, 7, 11, 12

<i>Finjan, Inc. v. Blue Coat Sys.</i> , 879 F.3d 1299 (Fed. Cir. 2018).....	5, 10
<i>Frybarger v. Salemme</i> , No. 22-61437-CIV-DIMITROULEAS, 2022 U.S. Dist. LEXIS 237087 (S.D. Fla. Dec. 28, 2022)	16
<i>Gesture Tech. Partners, LLC v. LG Elecs. Inc.</i> , No. 21-19234 (SRC), 2024 U.S. Dist. LEXIS 231623 (D.N.J. Dec. 23, 2024)	8
<i>In re Killian</i> , 45 F.4th 1373 (Fed. Cir. 2024)	15
<i>Intell. Ventures I LLC v. Erie Indem. Co.</i> , 134 F. Supp. 3d 877 (W.D. Pa. 2015).....	3
<i>Intell. Ventures I LLC v. Symantec Corp.</i> , 100 F. Supp. 3d 371 (D. Del. 2015).....	5
<i>Intell. Ventures I LLC v. Symantec Corp.</i> , 838 F.3d 1307 (Fed. Cir. 2016).....	5
<i>Knapp Med. Ctr. v. Burwell</i> , 192 F. Supp. 3d 129 (D.D.C. 2016)	4
<i>KOM Software Inc. v. NetApp, Inc.</i> , 697 F. Supp. 3d 203 (D. Del. Oct. 4, 2023)	12
<i>Luminati Networks Ltd. v. Code200, UAB</i> , No. 2:19-CV-00396-JRG, 2021 U.S. Dist. LEXIS 24742 (E.D. Tex. Feb. 9, 2021)	8
<i>Luminati Networks Ltd. v. Teso LT</i> , No. 2:19-cv-00395-JRG, 2021 U.S. Dist. LEXIS 28060 (E.D. Tex. Feb. 21, 2021)	12
<i>Mirror Imaging, LLC v. PNC Bank, N.A.</i> , No. W-21-CV-00518-ADA, 2022 U.S. Dist. LEXIS 13832 (W.D. Tex. Jan. 26, 2022).....	7
<i>Mobile Acuity Ltd. v. Blippar Ltd.</i> , 110 F.4th 1280 (Fed. Cir. 2024)	2
<i>MyMail, Ltd. v. ooVoo, LLC</i> , 934 F.3d 1373 (Fed. Cir. 2019).....	18
<i>Nat. Alternatives Int'l, Inc. v. Creative Compounds, LLC</i> , 918 F.3d 1338 (Fed. Cir. 2019).....	19
<i>Opensesame, Inc. v. GoI Pty, Ltd.</i> , No. 3:21-cv-1258-AR, 2025 U.S. Dist. LEXIS 102975 (D. Or. May 30, 2025)	15
<i>PalTalk Holdings, Inc. v. Riot Games, Inc.</i> , No. 16-1240-SLR, 2017 U.S. Dist. LEXIS 73181 (D. Del. May 15, 2017).....	6
<i>Prism Techs. LLC v. T-Mobile USA, Inc.</i> , 696 F. App'x 1014 (Fed. Cir. 2017).....	12

<i>Redwood Techs., LLC v. Netgear, Inc.</i> , No. 22-1272-GBW, 2024 U.S. Dist. LEXIS 195912 (D. Del. Oct. 28, 2024)	8
<i>Sec. First Innovations, LLC v. Google LLC</i> , No. 2:23-cv-97, 2023 U.S. Dist. LEXIS 205040 (E.D. Va. Nov. 15, 2023)	4, 6
<i>Slyce Acquisition Inc. v. Syte – Visual Conception Ltd.</i> , No. W-19-CV-00257-ADA, 2020 U.S. Dist. LEXIS 9451 (W.D. Tex. Jan. 10, 2020)	18
<i>TaKaDu Ltd. v. Innovyze, Inc.</i> , No. 21-291-RGA, 2022 U.S. Dist. LEXIS 40614 (D. Del. Mar. 8, 2022)	11
<i>Tefera v. OneWest Bank, FSB</i> , 19 F. Supp. 3d 215 (D.D.C. 2014)	3
<i>Tew v. Thomas</i> , No. 10-00511 LEK, 2011 U.S. Dist. LEXIS 13335 (D. Haw. Feb. 9, 2011)	2
<i>TimePlay, Inc. v. Audience Entm't LLC</i> , No. 15-05202 SJO (JCx), 2015 U.S. Dist. LEXIS 174781 (C.D. Cal. Nov. 10, 2015)	3
<i>Ultramercial, Inc. v. Hulu, LLC</i> , 722 F.3d 1335 (Fed. Cir. 2013)	18
<i>Vampire Fam. Brands, LLC v. MPL Brands, Inc.</i> , No. 20-9482-DMG (ASx), 2021 U.S. Dist. LEXIS 174965 (C.D. Cal. Aug. 6, 2021)	2
<i>Voiceage Evs. LLC v. HMD Glob. Oy</i> , No. 19-1945-GBW, 2025 U.S. Dist. LEXIS 92569 (D. Del. May 14, 2025)	3, 7, 14, 17
<i>WSOU Invs. v. Netgear, Inc.</i> , No. 21-1119-MN-CJB, 2022 U.S. Dist. LEXIS 124612 (D. Del. July 14, 2022)	12
Statutes	
Conn. Gen. Stat. § 19a-131 (2025)	4
Rules	
Fed. R. Civ. P. 56	3

I. INTRODUCTION

The claims of asserted U.S. Patent No. 8,234,705 ("the '705 Patent") are directed to a technological solution to a technical problem that improves the security of a protected computer network and cannot legally be considered as being directed to an abstract idea under *Alice*-Step 1. *See generally Alice Corp. Pty. Ltd. v. CLS Bank Int'l*, 573 U.S. 208 (2014). These claims further include an inventive concept that goes far beyond the mere "idea" of protecting a computer network from malware¹ and thus also cannot properly be considered, as a matter of clear and convincing fact, as failing *Alice* Step 2. In their Motion to Dismiss Plaintiff K.Mizra LLC's ("K.Mizra") Complaint (ECF No. 19, the "Motion"), Defendants Citrix Systems, Inc. and Cloud Software Group, Inc. (collectively "Citrix") fail to prove otherwise.

Citrix's attempt to invalidate the '705 Patent relies on a gross-oversimplification of the claimed inventions. First, the Motion attempts to minimize to nonexistence the importance of several critical claim elements. (Motion at 15, 17-18.) Then, it ignores the claim language altogether in favor of focusing on a general description of the claims. (*Id.* at 3-5, 16.) Citrix finally, aided by an ill-explained and confusing analogy, asserts that the '705 Patent's claims are directed not towards a unique system to protect a computer network from other computers trying to harm it, an obvious improvement in computer network security technology, but rather towards methods for requiring vaccinations for school attendance. (*Id.*)

In short, Citrix fails to meet its burden to provide a sufficient analysis of the issues under the two-part *Alice* test. But even if Citrix had performed a bare minimum analysis, the Court should still conclude, at this point in the proceedings, that the Motion cannot be granted under the required clear and convincing evidence standard. Indeed, that is exactly what another district court was compelled to find, but unlike here, not on a motion to dismiss, but at summary judgment, granting K.Mizra's motion and dismissing just prior to trial the then-asserted 35 U.S.C. § 101 defense.

II. APPLICABLE LEGAL STANDARDS

Courts apply a two-step test, commonly referred to as the *Alice* test, to determine whether a patent claims patent-ineligible subject matter. *Alice*, 573 U.S. at 217-218. At *Alice*-Step one,

¹ "Malware" is a catch-all term for various malicious software, including viruses, adware, spyware, browser hijacking software, and fake security software. Once installed on a computer, these programs can migrate to other computers to which the infected computer is networked and can seriously affect privacy and security of the entire network.

courts determine whether a claim is directed to a patent-ineligible concept such as an abstract idea. *Broadband iTV, Inc. v. Amazon.com, Inc.*, 113 F.4th 1359, 1367 (Fed. Cir. 2014). "If not, the inquiry ends." *Id.* Otherwise, the analysis proceeds to step two, where courts review "whether the [challenged] claim recites elements sufficient to transform it into a patent-eligible application of the abstract idea." *Id.* Citrix bears the burden of proving that the claims of the '705 Patent are invalid under Section 101 under the clear and convincing standard and that burden never shifts. *See Mobile Acuity Ltd. v. Blippar Ltd.*, 110 F.4th 1280, 1290 (Fed. Cir. 2024). Citrix has not and cannot meet its heavy burden.

III. ARGUMENT

A. A Federal Court Has Already Found These Claims Patent Eligible

As Citrix acknowledges, K.Mizra filed a summary judgment motion on this exact defense in *K.Mizra LLC v. Hewlett Packard Enterprise Company et al. ("HPE")*, No. 2:21-cv-00305-JRG (E.D. Tex.) (ECF No. 19-3). Prior to trial and apparently recognizing the futility of the defense², HPE withdrew its claim of patent invalidity under 35 U.S.C. § 101. (Declaration of Brian Boerman ("Boerman Decl.") filed concurrently herewith, ¶ 4, Ex. A.) But what Citrix neglects to mention in its Motion is that in *K.Mizra LLC v. Cisco Systems, Inc. ("Cisco")*, No. 6:20-cv-01031-ADA (W.D. Tex.), Cisco also asserted a Section 101 defense to the charge of infringing the '705 Patent. (Boerman Decl., ¶ 5.) But unlike HPE, Cisco did not withdraw the defense. Rather, K.Mizra was forced to move for summary judgment thereon. (*Id.* ¶ 6, Ex. B.)³ The Court granted that motion (*id.* ¶ 7, Ex. C), finding that the exact defense asserted here failed "as a matter of law," Fed. R.

² No competent attorney would abandon a meritorious defense—particularly one it was entitled to as a matter of law. Indeed, such action could be considered ineffective assistance of counsel in the criminal law context. *See, e.g., Tew v. Thomas*, No. 10-00511 LEK, 2011 U.S. Dist. LEXIS 13335, at *9 n.11 (D. Haw. Feb. 9, 2011). HPE was represented by Sean Cunningham of DLA-Piper, a highly skilled and well respected IP litigator, certainly more than merely competent. *See* Sean C. Cunningham, <https://www.dlapiper.com/en-us/people/c/cunningham-sean-c>, DLA Piper (last visited June 24, 2025).

³ The Court may take judicial notice of filings in other cases involving the '705 Patent. *Vampire Fam. Brands, LLC v. MPL Brands, Inc.*, No. 20-9482-DMG (ASx), 2021 U.S. Dist. LEXIS 174965, at *3 (C.D. Cal. Aug. 6, 2021) ("Court filings and orders issued in related litigation are [] proper subjects of judicial notice").

Civ. P. 56(a). These events directly contradict Citrix's claim that it is entitled to a finding that the '705 Patent is invalid as a matter of law, especially on a motion to dismiss.⁴

B. The '705 Patent Claims Are Not Directed To An Abstract Idea (*Alice*-Step 1)

Citrix has failed to satisfy its burden to establish that the claims of the '705 Patent are directed to an abstract idea. First, Citrix fails to prove that what it asserts to be the "idea" of the challenged claims is in fact "abstract." Second, Citrix fails to prove that the claims of the '705 Patent are even actually directed to what it proposes is an "abstract idea." These failures are likely due to the fact that when examined closely, the language of the claims confirms that they are directed to a technological solution to a technological problem, rather than an abstract idea.

1. Citrix Fails to Establish that the Claims are directed to an Abstract Idea

Citrix bears the burden of proving that the '705 Patent's claims are directed to a specific and well-defined abstract idea, often by analogy and as a matter of law. *Voiceage Evs. LLC v. HMD Glob. Oy*, No. 19-1945-GBW, 2025 U.S. Dist. LEXIS 92569, at *22 (D. Del. May 14, 2025). Citrix has failed to present a cogent explanation of the "abstract idea" to which the '705 Patent claims are allegedly directed or provide an analogy that shows legal abstractness, meaning its motion fails as a matter of law at *Alice*-Step 1. *See, e.g., TimePlay, Inc. v. Audience Entm't LLC*, No. 15-05202 SJO (JCx), 2015 U.S. Dist. LEXIS 174781, at *18 (C.D. Cal. Nov. 10, 2015) ("Defendant has not pointed to any authority compelling the conclusion that [the identified idea in the motion] . . . is 'abstract' within the meaning of Section 101").

The Motion is unclear on what "abstract idea" is allegedly captured by the claims. The Motion initially states that "the human practice of quarantine is ancient," calling to mind the practice of isolating possibility infected from those people known to be uninfected. (Motion at 3;

⁴ The '705 Patent has been asserted in eleven prior federal court actions and, it is only in this case, where a defendant has moved to have the Patent found invalid as a matter of law. (Boerman Decl. ¶¶ 8-9.) This is true even though such motions have become pro forma on any claim with any chance of being invalidated on this basis—one court described *Alice* as having opened "the proverbial motions practice floodgates" and noted that Section 101 issues were "being litigated daily (if not hourly) in federal courts across the country." *Intell. Ventures I LLC v. Erie Indem. Co.*, 134 F. Supp. 3d 877, 895 (W.D. Pa. 2015), *vacated in part* by 850 F.3d 1315 (Fed. Cir. 2017). The Court may and should take judicial notice of the existence of these other cases and their procedural settings and lack of defendant initiated Section 101 motions practice. *See, e.g., Tefera v. OneWest Bank, FSB*, 19 F. Supp. 3d 215, 220 (D.D.C. 2014) (noting that courts may take judicial notice of "the existence of other litigations").

Boerman Decl., Ex. D ("Quarantine separates and restricts the movement of people who *were exposed* to a contagious disease to see if they become sick.") (emphasis added).)⁵ Indeed, this definition is consistent with how the term is used in public health statutes. *See, e.g.*, Conn. Gen. Stat. § 19a-131(9) (2025) (defining "quarantine" with reference to individuals "who *are exposed* to a communicable disease . . ." (emphasis added)). But the Motion then pivots to discussing, instead of quarantining, the different idea of "immunization against communicable diseases." (Motion at 3.) Immunization requires preventive action be taken *before* exposure and/or infection, making quarantine of an immunized individual unnecessary. Citrix then further confuses the issue by later stating that "the essential premise of quarantine is a blanket exclusion of unverified entities due to potential exposure to the unknown (Motion at 19), which does not appear to match up either with traditional understandings of quarantine (how are people who have been exposed to infectious diseases "unverified entities") or immunization (how could vaccines work against an "unknown" disease). So, and again, it is unclear to K.Mizra how immunization relates to the "ancient" practice of quarantining, either generally in human experience, or certainly in the context of computer network security.

Citrix next contends that the claims are directed to the abstract idea of "protecting a network from an infected host through contagion isolation and inoculation." (Motion at 10.) It alleges that this is the same as "the human practice of quarantining" in response to medical emergencies such as "the global pandemic experienced in recent years." (*Id.* at 3.) Citrix then points to a 2004 Florida statute related to checking immunizations of an individual before permitting entry of that individual to a school. (*Id.* at 3-5.) But even if this allegedly abstract idea were accepted by the Court, the analogy does not here work. A party alleging invalidity cannot merely point to *any* analogy to support its "abstract idea" analysis. *See, e.g., DDR Holdings, LLC v. Hotels.com, L.P.*, 773 F.3d 1245, 1258 (Fed. Cir. 2014) (rejecting analogy where context "introduces a problem that does not arise in the 'brick and mortar' context"); *Data Engine Techs. Ltd. v. Google LLC*, 906 F.3d 999, 1011 (Fed. Cir. 2018) ("It is not enough, however, to merely trace the invention to some real-world analogy."); *Sec. First Innovations, LLC v. Google LLC*, No. 2:23-cv-97, 2023 U.S. Dist. LEXIS 205040, at *42 (E.D. Va. Nov. 15, 2023) (noting that a claim "is not abstract just because

⁵ The Court may take judicial notice of information on HHS's website. *See Knapp Med. Ctr. v. Burwell*, 192 F. Supp. 3d 129, 131 n.1 (D.D.C. 2016).

it can be analogized to something that can be done in the physical world"). Rather, the analogy must be focused on the problem actually being addressed by the claimed invention.

The Federal Circuit decision in *DDR Holdings* is particularly instructive here, as it notes that a problem with the analogy in that case was that it failed to account for "the ephemeral nature of an Internet 'location' or the near-instantaneous transport between these locations." *DDR Holdings*, 773 F.3d at 1258. Similarly, computer network security presents a host of problems that do not arise in the medical context, several of which are highly relevant to the issues addressed by the '705 Patent. For instance, the '705 Patent specifically notes that software may be installed on a host computer by the operator of the protected network for the protection of the host and/or network. '705 Patent at 1:25-28. Citrix would apparently liken this to a vaccine. But the medical field does not have to deal with situations where the vaccine is "removed or altered without authorization," as is the case in the computer security field. *Id.* at 1:28. In at least that way (and there are others), detecting an insecure condition on a host is significantly different from checking whether a person has received a vaccine.

Indeed, courts have repeatedly recognized that differences between computer security and medicine make such comparisons unhelpful. For example, in *Intell. Ventures I LLC v. Symantec Corp.*, the Federal Circuit found that the claim involved computer virus screening. 838 F.3d 1307, 1361 (Fed. Cir. 2016). But neither the Federal Circuit nor the district court below relied on the widespread use of *medical tests* to check for *diseases in humans* to assess whether the claimed computer network virus screening inventions were abstract. (*Id.*; see also *Intell. Ventures I LLC v. Symantec Corp.*, 100 F. Supp. 3d 371, 402 (D. Del. 2015) (district court rejecting analogy of virus screening to, among other things, "observing individuals for signs of intoxication").) Although the Federal Circuit overturned the district court's abstractedness conclusion, it did so not based upon an analogy to medical concepts, but on well-known and prior art computer network technologies.

Another instructive computer security case is *Finjan, Inc. v. Blue Coat Sys.*, where the Federal Circuit acknowledged that virus scanning generally was an abstract idea, but holding that the claims of the Finjan patent were not directed to that abstract idea but rather to a "'behavior-based' approach to virus scanning." 879 F.3d 1299, 1303-04 (Fed. Cir. 2018). Similarly, here, the '705 Patent's claims are not directed to mere "virus scanning" but rather to a comprehensive system for protecting a computer network from malware that may be installed on a host computer from

migrating to the network *and* for rendering the host computer clean. *Finjan* precludes the analytical approach suggested by Citrix.

To put a finer point on why Citrix's *Alice*-Step 1 analysis fails as a matter of law, we need to look at Citrix's *Alice*-Step 2 analysis, where it compares a claimed web server request to a child arriving at the entrance of a school, an immunization clinic to the claimed quarantine notification page, a sick child calling a school to ask for the school's address to the claimed DNS query, and an address for the immunization clinic to the claimed IP address for a quarantine server. (Motion at 18.) Obviously, an immunized child is not akin to a secure computer network, and if analogizing one to the other were appropriate to prove abstraction, no patent claims to the computer security arts would ever pass a Section 101 analysis and many obviously do. The approach employed by Citrix is just legally wrong. *See Sec. First Innovations*, 2023 U.S. Dist. LEXIS 205040, at *42 (showing how claims confirmed by the Federal Circuit could be found abstract using this approach).

Finally, Citrix cites *Ericsson, Inc. v. TCL Commc'n Tech Holdings Ltd.* to support its "abstract idea" analogy argument. (Motion at 16.) But *Ericsson* requires a showing that the abstract idea analogy evidence "predates the [challenged patent] and is pervasive in human activity." 955 F.3d 1317, 1327 (Fed. Cir. 2020). Here, the only evidence that Citrix mentions, beyond a vague reference to "quarantining," is a 2004 Florida statute. (Motion at 3-5.) As a preliminary matter, this argument fails at the motion to dismiss stage because it is necessarily based on extrinsic evidence. *Accord. PalTalk Holdings, Inc. v. Riot Games, Inc.*, No. 16-1240-SLR, 2017 U.S. Dist. LEXIS 73181, at *12 (D. Del. May 15, 2017) ("Absent clear direction from the specification, the prosecution history, or the pleadings, a comparison or analogy . . . could [only] enter the record through extrinsic evidence" that would "constitute matter beyond the pleadings"). But even if the Court could consider the statute, it still cannot support Citrix's burden. After all, as Citrix acknowledges, the statute is from the same year as the provisional application from which the '705 Patent issued and to which it claims priority. (Motion at 3.)⁶ In other words, Citrix fails to show that the Florida statute "predates" the '705 Patent. Citrix also fails to address the broader points raised by *Ericsson*: whether the alleged abstract idea "is exactly the sort of process that can be

⁶ The Provisional Application was filed on September 27, 2004. (ECF No. 1-4 at 1.) No specific date is identified for publication of the Florida statute offered by Citrix, and it well could have not been public until well after September 27, 2004. (ECF No. 19-1.)

performed in the human mind, or by a human using a pen and paper." *Ericsson*, 955 F.3d at 1327. This is not surprising, because it cannot.

For any one of these three reasons, Citrix has not proved by clear or convincing evidence that the asserted '705 patent claims encompass a legally "abstract concept." But that is not all, there are several other reasons these claims cannot be considered "abstract" under *Alice*-Step 1, as a matter of law.

2. Citrix Fails to Establish That the Actual Claim Language Meets its Proposed Abstract Idea Definition

At *Alice*-Step 1, Citrix additionally bears the burden of establishing that the *claims* are directed at the proposed abstract idea. See *Voiceage*, 2025 U.S. Dist. LEXIS 92569, at *22 ("To meet its burden at *Alice* step one, Defendant must propose an abstract idea that fairly characterizes the Challenged Claims and thus avoids oversimplifying the Challenged Claims."). Indeed, "[t]he focus must remain on the claim language" because "overgeneralizations can almost always create a high level of abstraction." *Mirror Imaging, LLC v. PNC Bank, N.A.*, No. W-21-CV-00518-ADA, 2022 U.S. Dist. LEXIS 13832, at *19 (W.D. Tex. Jan. 26, 2022) (citing *TecSec, Inc. v. Adobe Inc.*, 978 F.3d 1278, 1292-93 (Fed. Cir. 2020)). Yet in the five pages of its Step 1 analysis (Motion at 11-16), Citrix barely mentions the language of the '705 Patent claims. It mentions the term "trusted computing base" once on page 12, but only to allege that it is mere jargon that may be ignored. (Motion at 12.) It also mentions certain terms to allege that they are generic computer components. (Motion at 15.) But Citrix never once addresses precise claim language to explain how its proposed abstract idea fairly characterizes that language.⁷ By focusing on a *summary* of the claims rather than the *claim language* itself, Citrix does exactly what the Federal Circuit says it cannot: "describing the claims at a high level of abstraction, divorced from the claim language itself." *Contour IP Holding LLC v. GoPro, Inc.*, 113 F.4th 1373, 1379 (Fed. Cir. 2024). Such an approach "all but ensures that the exceptions to § 101 swallow the rule." *Id.* at 1380.

⁷ Perhaps nodding towards its burden, Citrix makes a broad statement that "every single element of the claims, including directing a host towards sources for obtaining inoculation and automation of the isolation process, is mirrored by the age-old process of restricting access to potentially infected hosts through quarantine." (Motion at 16.) But to support this statement, it references Section II.B of the Motion which, again, fails to address the claim language. (*Id.* at 3-5.) Instead, it focuses on a broad description of the claims provided in the Complaint, which is particularly puzzling given that Citrix also claims that these allegations are mere legal conclusions that should be ignored. (*Id.* at 9 n.3.)

Indeed, courts frequently reject Section 101 challenges where defendants fail to properly consider the language of the claim. For example, in *Redwood Techs., LLC v. Netgear, Inc.*, a district court found that Netgear failed to meet its burden on *Alice*-Step 1 because its opening brief "lack[ed] sufficient discussion of [the relevant claim] limitations," which was "problematic, as the focus must ultimately be on the claim language itself." No. 22-1272-GBW, 2024 U.S. Dist. LEXIS 195912, at *12 (D. Del. Oct. 28, 2024). In *Gesture Tech. Partners, LLC v. LG Elecs. Inc.*, another district court found that LG failed to meet its burden by "not merely oversimplify[ing] claim 4 but ignor[ing] all the details set forth in claims 1 and 4." No. 21-19234 (SRC), 2024 U.S. Dist. LEXIS 231623, at *6 (D.N.J. Dec. 23, 2024). Indeed, by refusing to address the actual claim language, Citrix also necessarily "fail[ed] to account for particular steps in the claims." *Luminati Networks Ltd. v. Code200, UAB*, No. 2:19-CV-00396-JRG, 2021 U.S. Dist. LEXIS 24742, at *14 (E.D. Tex. Feb. 9, 2021).

3. The '705 Patent Claims are Directed to a Technological Solution to a Technological Problem

The Federal Circuit has recognized that claims directed at improvements in the operation of a computer are not abstract. In other words, the "abstract idea" inquiry "often turns on whether the claims focus on the asserted improvement in computer capabilities or, instead, on a process that qualifies as an abstract idea for which computers are invoked merely as a tool." *Ancora Techs. v. HTC Am., Inc.*, 908 F.3d 1343, 1347 (Fed. Cir. 2018). The Federal Circuit has further acknowledged that "[i]mproving security . . . can be a non-abstract functionality improvement if done by a specific technique that departs from earlier approaches to solve a specific computer problem." *Id.* at 1348. That is here the case.

As explained in the '705 Patent, existing methods of accessing remote networks had significant security problems arising from vulnerabilities of a remote host computer. '705 Patent at 1:14-41. It explained that the remote hosts may pose a danger to elements of a protected network when they "reconnect [to the protected network] after a period of connection to one or more networks and/or systems that are not part of the [] protected network." *Id.* at 1:19. These threats include software installed on the remote host to protect the protected network may be removed or altered, or configurations, settings, and security data may be added, removed, or changed in unauthorized ways. *Id.* at 1:25-31. Upon connecting to the protected network, these threats may infect and/or harm the protected network "before measures can be taken to detect and prevent the spread of such infections or harm." *Id.* at 1:34-38. The claims of the '705 Patent are accordingly

related to "a reliable way to ensure that a system does not infect or otherwise harm other network resources when connected to a protected network." *Id.* at 1:38-41. The claims of the '705 Patent are directed at a technological solution to these then-existing technological problems and the claimed inventions improve the security of the protected network. (*Accord.* ECF No. 1 ¶ 33 (noting that the asserted claims are directed to a machine-implemented solution resolving a machine-implemented problem).)

For example, claim 19 of the '705 Patent recites, among other things, "detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network." By checking the security status of the remote host before connecting to the protected network or allowing the connected host to access network resources, the claimed invention catches security threats that were not addressed in previously known network security solutions. The '705 Patent also specifically calls out threats when a host *reconnects* to the protected network after "software installed on the mobile system by an operator of the protected network for the protection of the mobile system and/or the protected network [is] removed or altered without authorization." '705 Patent at 1:25-28. But the claimed system would catch these threats, as it confirms the security status of the host upon each reconnection rather than relying on the preventive measures offered by the original software installation. Importantly, this solution is implemented by "contacting a trusted computing base associated with a trusted platform module within the first host, receiving a response, and determining whether the response includes a valid digitally signed attestation of cleanliness." '705 Patent, claim 19. In this way, the claimed system provides a real-time view of the security status of the host computer, rather than relying on previously-implemented preventive security measures that may have been compromised between connection sessions. The claimed system also ensures network security by using real-time information received from the trusted computing base/trusted computing module, which are secure hardware components installed on the host system and less vulnerable to attack and thus reliably provide real-time information about the security status of the host computer. (*See* ECF No. 1 ¶ 31 (emphasizing the use of tamperproof hardware to protect the secure computer network). In this manner, the security of the protected network is improved through the specific way in which it implements the quarantine and remediation process, all technological concepts specifically claimed in the '705 Patent.

Comparable cases related to computer security (rather than general access restriction cases) confirm the patentability of the claims of the '705 Patent. For instance, in *Finjan*, the Federal

Circuit addressed claims involving a "behavior-based" approach to virus scanning. 879 F.3d at 1304. On its face, the reviewed claim of that patent is more general than the claims at issue here:

[Preamble] A method comprising:

[A] receiving by an inspector a Downloadable;

[B] generating by the inspector a first Downloadable security profile that identifies suspicious code in the received Downloadable; and

[C] linking by the inspector the first Downloadable security profile to the Downloadable before a web server makes the Downloadable available to web clients.

But the Federal Circuit had no problem concluding that this claim was not directed to an abstract idea, explaining that traditional systems only looked for the presence of known viruses, but that the claimed solution addressed the weakness of this prior approach by protecting against previously unknown viruses as well as "obfuscated code," *i.e.*, known viruses that have been modified to avoid detection. *Id.* The improved ability to detect viruses, which was implemented with specific steps in the *Finjan* claims, resulted in a finding that the claims were non-abstract. *Id.* at 1305-06. The claims here are likewise non-abstract for the same reason: they provide a new approach to computer security that enhances protection of the overall networked computer system.

The Federal Circuit's decision in *Ancora* is likewise informative, with the claims there dealing with verification of licenses:

[Preamble] A method of restricting software operation within a license for use with a computer including an erasable, non-volatile memory area of BIOS of the computer, and a volatile memory area; the method comprising the steps of:

[A] selecting a program residing in the volatile memory;

[B] using an agent to set up a verification structure in the erasable, non-volatile memory of the BIOS, the verification structure accommodating data that includes at least one license record,

[C] verifying the program using at least the verification structure from the erasable non-volatile memory of the BIOS, and

[D] acting on the program according to the verification.

Ancora, 908 F.3d at 1345-46. The district court observed that storing the verification structure in BIOS "calls for nothing more than storing data in the memory of a computer component that generally stores data." *Id.* at 1346. In reversing the district court's invalidity finding, the Federal

Circuit found that the claim was not directed to an abstract idea because use of the BIOS in this new context "results in a beneficial reduction to the risk of hacking." *Id.* at 1349.⁸ As explained above, use of the "trusted computing base," which is part of the "trusted computing module," in the particular way claimed in the '705 Patent likewise results in a beneficial improvement in the security of the protected network. (See ECF No. 1 ¶ 31 (emphasizing that the specific tamperproof hardware "interact[s] with unique software to improve network access control technology and protect a secure computer network and the data stored thereon from infected devices").)

Another question courts may consider in determining claim abstraction is whether the claims recite mental processes that may be performed by a human. *Ericsson*, 955 F.3d at 1327. But the '705 Patent's claims focused on specific computer security systems and are not akin to the recitation of mental processes, and Citrix has not suggested otherwise. See *TaKaDu Ltd. v. Innovyze, Inc.*, No. 21-291-RGA, 2022 U.S. Dist. LEXIS 40614, at *16 (D. Del. Mar. 8, 2022). To be sure, the improvements identified above are not the only way in which the '705 Patent's claims represent an improvement to the operation of a computer (or, as here, to a network of computers). As described in the Complaint, for example, the claims of the '705 Patent also advantageously "allow[s] a machine to automatically and dynamically select and isolate an unsafe device attempting to access a secure network" and thus "remov[es] the once-necessary human intervention from a fundamentally mechanical process." (ECF No. 1 ¶ 32.) Such an automatic process is vital to security where "a system may infect or otherwise harm resources associated with the protected network ***before measures can be taken to detect and prevent the spread of infections or harm.***" '705 Patent at 1:36-38 (emphasis added). Requiring human intervention would only serve to delay these measures and increase the danger to the protected network, again meaning the claimed systems cannot properly be considered abstract.

⁸ Citrix makes much of the "admission" in the specification of the '705 Patent that trusted computing modules ("TCM") existed before the invention. (Motion at 3.) But while that is true, these TCMs were not, prior to the invention of the '705 Patent, used as claimed in the Patent and, as *Ancora* demonstrates, the prior existence of a system component is not conclusive in the *Alice* inquiry. Rather, the issue is novelty and there is no evidence in this record that TCMs were previously used to improve security of protected networks in the same way as claimed in the '705 Patent.

4. Citrix's Relied-Upon Access Control Cases Demonstrate Non-Abstraction

Citrix relies heavily here on *Ericsson*, a case where the Federal Circuit found the involved claims collapsed into nothing more than "simply 'an access controller for controlling access' by 'receiving a request' and then 'determining if the request should be granted.'" 955 F. 3d at 1326. Unlike the claims at issue here, there was no explanation for how the claim provided an improvement over existing methods of access control, with the Federal Circuit specifically noting that the "claims are silent as to **how** access is controlled." *Id.* at 1328 (emphasis added). The claims of the '705 Patent specifically do explain how to keep a computer network secure and other district courts have recognized that *Ericsson* is unhelpful where the claims address, as here, implementation of the claimed invention, *WSOU Invs. v. Netgear, Inc.*, No. 21-1119-MN-CJB, 2022 U.S. Dist. LEXIS 124612, at *9-10 (D. Del. July 14, 2022) (claims about more particular way of controlling access to resources), or where, as here, the claims are not directed to an idea that could be implemented with pen and paper, *Luminati Networks Ltd. v. Teso LT*, No. 2:19-cv-00395-JRG, 2021 U.S. Dist. LEXIS 28060, at *15 (E.D. Tex. Feb. 21, 2021) (distinguishing *Ericsson* because an improvement in network design that addresses congestion "is not something a human being can perform using a pen and pad"). Indeed, Citrix's assertion that the '705 Patent's claims are similar to the claims in *Ericsson* because they "concern[] granting access to a network based on particular criteria," is, at best, yet another gross overgeneralization of what the claims here are actually about.

Citrix also relies on *Prism Techs. LLC v. T-Mobile USA, Inc.*, although it neglects to mention that the opinion is non-precedential. 696 F. App'x 1014 (Fed. Cir. 2017). Again, this case concerns a claim directed to "providing restricted access to resources," which recited generic steps such as receiving identity data, confirming the identity data, determining that the device was authorized, and permitting access to the resources if authorized. *Id.* at 1017. Although Prism alleged that the claims cover a concrete solution to a real-world problem, the Court noted that it did "not proffer a persuasive argument in support of this conclusion." *Id.* Other district courts have recognized that Prism "claimed the function of a computer permitting access to resources **by any means** that determined that the request for resources was permitted." *KOM Software Inc. v. NetApp, Inc.*, 697 F. Supp. 3d 203, 215 (D. Del. Oct. 4, 2023) (emphasis added). They did not, however, "recite the mechanics of an authentication process," as is here the case. *Id.*

Finally, Citrix cites to an out-of-district opinion from 2017 that does not appear to have been cited by any other court in the last eight years. *See Dist. Media Techs., Inc. v. Hulu, LLC*, No. 4:16cv245-MW/CAS, 2017 U.S. Dist. LEXIS 179660 (N.D. Fla. July 3, 2017). This decision provides a limited explanation of its *Alice*-Step 1 analysis and indeed did not even identify the abstract idea to which it believed the claims were directed. *Id.* at *9-10. Regardless of the precise abstract idea, though, the court noted that the claims at issue did "little more than recite an abstract idea (delivering content secured with licenses and encryption) with the instruction to perform it on generic computer components." *Id.* at *13. The district court then went on to specifically distinguish another case finding non-abstract claims using "specific and non-generic 'trusted' devices and systems." *Id.* at *14. Citrix should not be allowed to gloss over these differences through a conclusory assertion that the claims are "remarkably similar" to the claims of the '705 Patent. (Motion at 13.)

Indeed, Citrix's treatment of all these cases suffers from the same problem as the rest of its analysis: it is superficial and fails to address the claim language here at issue. At some level, it is true, the '705 Patent's claims address access control, or at least whether a remote host may be allowed to send data to or receive data from a protected network.⁹ But as the Supreme Court has observed, "[a]t some level, all inventions embody, use, reflect, rest upon, or apply . . . abstract ideas." *Alice*, 573 U.S. at 217. That alone does not make the claimed invention abstract. More is needed to hold as a matter of law a claimed invention abstract and Citrix provides little if any explanation for why it believes the claims addressed in these allegedly-analogous cases are relevant to the Court's analysis of the '705 Patent's claims, which is fatal to its *Alice*-Step 1 analysis.

C. The Claims Include An Inventive Concept (*Alice*-Step 2)

The claims of the '705 Patent also include an inventive step, which provides an independent basis for the Court to deny Citrix's Motion. Of course, analysis of whether the claims include an inventive concept is unnecessary here, as Citrix has not proven by clear and convincing evidence that the '705 Patent's asserted claims encompass nothing but an abstract idea. *Broadband iTV*, 113 F.4th at 1367. But for completeness, K.Mizra will now show why these claims also pass *Alice*-Step 2. Claims are patentable at step two if they describe a solution that is "necessarily rooted in computer technology in order to overcome a problem specifically arising in the realm of computer

⁹ It is less clear why Citrix believes the claims of the '705 Patent related to authentication or authorization. (Motion at 13-14.)

networks." *DDR Holdings, LLC*, 773 F.3d at 1257; *see also Amdocs (Isr.) Ltd. v. Openet Telecom, Inc.*, 841 F.3d 1288, 1294 (Fed. Cir. 2016) (noting "there is considerable overlap between step one and step two"). Indeed, courts have specifically found that a "technological solution to a technological problem"—often considered to demonstrate the claims are not directed to an abstract idea at step one—may also provide the "something more" to qualify as an inventive concept at the step 2 inquiry, which is here the case. *Amdocs*, 841 F.3d at 1301.

The '705 Patent's claims address the security vulnerabilities in protected networks caused by potentially-infected host computers that seek to connect with the protected network. (*See supra* Section III.B.3.) The '705 Patent then describes a specific solution to this specific computer network security problem and that claimed solution is necessarily rooted in computer technology, by (for example) contacting a trusted computing base located within the host computer and receiving in response an attestation of cleanliness that provides a real-time and secure view of the security of the connecting host. This in turn allows the protected network to quarantine compromised hosts based on the real-time and secure view of its security. As a whole, then, the claimed invention improves the ability of the protected network to quarantine and remediate infected devices while allowing uninfected devices to access the network. In this manner, and in the context of the claimed ordered combination of claim elements (*see* ECF No. 1 ¶ 33), the claims of the '705 Patent provide a technological solution to a technological problem and improve the operation of the protected network by increasing its security. *DDR Holdings*, 773 F.3d at 1259 ("When the limitations . . . of the claims are taken together as an ordered combination, the claims recite an invention that is not merely the routine or conventional use of the Internet."); *BASCOM Global Internet Servs. v. AT&T Mobility LLC*, 827 F.3d 1341, 1350 (Fed. Cir. 2016); *see also Voiceage*, 2025 U.S. Dist. LEXIS 92569, at *51.

The factual allegations here establish that this claimed ordered combination of elements is unconventional. For example, the Complaint alleges that "the Asserted Claims focus on specific tamperproof hardware [, the trusted computing module,] that must interact with unique software to **improve** network access control technology and protect a secure computer network and the data stored thereon from infected devices." (ECF No. 1 ¶ 31.) The allegation establishing that this ordered combination is an improvement on existing technologies and resolves the step two inquiry in K.Mizra's favor at this stage of the case. *Aatrix Software, Inc. v. Green Shades Software, Inc.*, 882 F.3d 1121, 1126-27 (Fed. Cir. 2018) ("*Aatrix I*") ("We have held that patentees who adequately

allege their claims contain inventive concepts survive a § 101 eligibility analysis under Rule 12(b)(6)."); *Opensesame, Inc. v. GoI Pty, Ltd.*, No. 3:21-cv-1258-AR, 2025 U.S. Dist. LEXIS 102975, at *7 (D. Or. May 30, 2025) (rejecting challenge at pleading stage where Complaint alleged "that its claimed invention is nonconventional and inventive.").

Citrix's arguments that the individual components of the claims are known (Motion at 17-18) are irrelevant to K.Mizra's pleaded ordered combination position, with the Federal Circuit finding an inventive step in a similar situation. *See Cosmokey Sols. GmbH & Co. AG v. Duo Sec. LLC*, 15 F.4th 1091 (Fed. Cir. 2021). In *Cosmokey*, the Federal Circuit agreed that the claims relied on conventional hardware. *Id.* at 1094. But the Federal Circuit nonetheless found an inventive concept because the ordered combination of elements (including software) "constitute an improvement that increases computer and network security." *Id.* at 1099; *see also BASCOM*, 827 F.3d at 1350 ("[A]n inventive concept can be found in the non-conventional and non-generic arrangement of known, conventional pieces."). The same is true here.

Citrix's broader point—that use of known trusted computing modules cannot provide an inventive concept even when used in a quarantine and remediation system to improve the security of a protected network—is also misplaced and directly contradicts *Ancora's* conclusion that use of known technology to improve existing verification procedures can indeed be a technological solution to a technological problem. *Ancora*, 908 F.3d at 1348. Although *Ancora* was addressing *Alice*-Step 1, the same issues are relevant and demonstrate that Citrix has also failed in its *Alice*-Step 2 analysis. *Amdocs*, 841 F.3d at 1301; *see also Cosmokey*, 15 F.4th at 1099 (relying on *Ancora* to support conclusion at step two).

The Federal Circuit has also noted that the preemptive effect of the claims asserted is a relevant consideration at *Alice*-Step 2. "[C]laims that recite a specific, discrete implementation of the abstract idea rather than preempting all ways of achieving an abstract idea using a computer may include an inventive concept." *In re Killian*, 45 F.4th 1373, 1382 (Fed. Cir. 2024). The claims at issue here do not preempt the proposed abstract idea of protecting a network from an infected host through contagion isolation and inoculation, which could clearly be accomplished without, *e.g.*, contacting a trusted computing base, receiving an attestation of cleanliness, or preventing communications with a host through use of a quarantine notification page, all as recited in

claim 19. True, such other methods of implementing contagion isolation and inoculation¹⁰ may not be as effective as the specific way recited in the '705 Patent, but that only serves to emphasize how the claims here include an inventive concept that is significantly more than Citrix's proposed abstract idea itself.

Citrix spends only one paragraph addressing whether the ordered combination of claim elements supplies an inventive concept. (Motion at 20.) But these conclusory arguments cannot meet Citrix's burden. For instance, Citrix claims that the combination does not supply an inventive concept because the patent describes components such as the "trusted platform module within the first host" as conventional components being used for their intended purpose. (*Id.*) The argument misses the mark, as it fails to consider how components such as the "trusted platform module" operate in the context of the claims as a whole. Indeed, Citrix's broad argument would also improperly capture the BIOS memory in *Ancora* which, after all, is only being used for its known function of securely storing data. *Ancora*, 908 F.3d at 1346.

Citrix next makes the conclusory statement that "the state of the art at the priority date of the '705 Patent already encompassed the ordered combination of its steps, which were widely recognized in ordinary human activities like school enrollment." (Motion at 20.) The argument is replete with flaws. First, it is a factual allegation regarding the state of the art, which raises factual issues that cannot be resolved on a motion to dismiss. *Chamberlain Yacht Sales, Inc. v. Phx. Glob. Equity Partners Ltd.*, No. 24-60953-CIV-DIMITROULEAS, 2025 U.S. Dist. LEXIS 80562, at *9 (S.D. Fla. Apr. 11, 2025) ("While a fact finder could ultimately agree with this conclusion, it is not for the Court to decide this factual issue on a motion to dismiss"). Second, the factual allegation is contradicted by the intrinsic record, as the examiner appeared to recognize that the ordered combination was unconventional. (Boerman Decl., Ex. E.) At this stage, all factual issues must be construed in the patentee's favor, including that the claimed invention issued by the United States Patent and Trademark Office is novel. *See Frybarger v. Salemm*, No. 22-61437-CIV-DIMITROULEAS, 2022 U.S. Dist. LEXIS 237087, at *15 (S.D. Fla. Dec. 28, 2022) ("When the plaintiff's complaint and supporting affidavits and evidence conflict with the defendant's affidavits,

¹⁰ In its *Alice*-Step 2 discussion, K.Mizra may adopt certain language suggested by Citrix's Motion. This is a recognition that *Alice*-Step 2 is irrelevant if Citrix is not correct at *Alice*-Step 1, and should not be understood as an indication that K.Mizra agrees with Citrix's overbroad characterization of the claims.

the Court construes all reasonable inferences in the plaintiff's favor."). Third, Citrix does not cite any factual support for its claim about the state of the prior art, so how can it meet its clear and convincing evidence burden? Fourth, to the extent that Citrix would rely on its step 1 analysis to support its step 2 burden, the argument merely inherits those flaws: Citrix does not address the claim language, relies on evidence outside the record, and does not even show that the school enrollment scheme is in the prior art. (*Supra* Sections III.B.1-2.) Finally, Citrix cannot resolve issues about the state of the art of computer security by referencing school enrollment, far outside the field of the relevant art. *See, e.g., Berkheimer v. HP Inc.*, 881 F.3d 1360, 1368 (Fed. Cir. 2018) (noting that the relevant question is "whether the claim element or claimed combination is well-understood, routine, conventional **to a skilled artisan in the relevant field**" (emphasis added)). Citrix's cursory analysis of the ordered combination of claimed elements alone is reason to deny the Motion. *See Voiceage*, 2025 U.S. Dist. LEXIS 92569, at *51 (finding step two burden not met where challenger "fail[ed] to adequately consider the elements of each claim both individually and as an ordered combination.").

Similarly, Citrix claims that elements [E], [E1], and [E2] of claim 19 amount to "conventional ways of re-routing internet traffic away from the protected network to a quarantine server." (Motion at 17.) But rather than supporting this assertion with reference to computer technology, Citrix relies on an analogy that compares a web server request to a sick child arriving at the entrance of a school and a DNS query to a sick child calling the school. (*Id.* at 18.) How these are comparable is left unexplained and they are obviously not comparable. Even if Citrix were able to justify its analogy some day with expert testimony, it has not done so here. Citrix also again attempts to prove conventionality by relying on an analogy far outside the relevant art. Moreover, Citrix appears to compare both the quarantine notification page and the quarantine server to an immunization clinic. (*Id.*) But Citrix elsewhere compares immunizations to remediation (*id.* at 5), which suggests Citrix instead believes that the immunization clinic is similar to the remediation host recited in element [F]. Citrix cannot rely on such a confused analogy to satisfy a clear and convincing evidence burden. *See Berkheimer*, 881 F.3d at 1368 ("Any fact, such as [whether a claim element or combination of elements is well-understood, routine and conventional], that is pertinent to the invalidity conclusion must be proven by clear and convincing evidence."). For at least this additional reason, Citrix failed to satisfy its burden to show the individual claimed elements are routine and conventional. *See Aatrix Software, Inc. v. Green*

Shades Software, Inc., 890 F.3d 1354, 1356 (Fed. Cir. 2018) ("Because the patent challenger bears the burden of demonstrating that the claims lack patent eligibility, 35 U.S.C. § 282(a), there must be evidence supporting a finding that the additional elements were well-understood, routine, and conventional.").

D. Subject Matter Eligibility Should Not Be Resolved On A Motion To Dismiss

As the Federal Circuit has recognized, "the analysis under § 101, while ultimately a legal determination, is rife with underlying factual issues." *Ultramercial, Inc. v. Hulu, LLC*, 722 F.3d 1335, 1339 (Fed. Cir. 2013) (vacated on other grounds). Here, factual disputes preclude a finding that the claims of the '705 Patent are invalid under Section 101. Indeed, the parties at the very least dispute whether the ordered combination described in claim 19 was unconventional. Coming to a conclusion on this issue involves underlying issues of fact that cannot be here resolved. *Cellspin Soft, Inc. v. Fitbit Inc.*, 927 F.3d 1306, 1315 (Fed. Cir. 2019) ("We have held that deciding whether claims recite an "inventive concept," or something more than "well-understood, routine, conventional activities previously known to the industry . . . may turn on underlying questions of fact."); *Ultramercial*, 722 F.3d at 1339 ("Almost by definition, analyzing whether something was "conventional" or "routine" involves analyzing facts."). It is thus common for courts to deny motions to dismiss where, as here, the complaint includes factual allegations that the elements of a claim are not well-understood, routine, or conventional activity, either individually or as an ordered combination. *See DeCurtis LLC v. Carnival Corp.*, No. 20-22945-Civ-SCOLA/TORRES, 2021 U.S. Dist. LEXIS 3163, at *32-36 (S.D. Fla. Jan. 6, 2021).

Moreover, courts have acknowledged that even without considering factual disputes, "resolving a patent's § 101 eligibility is rarely appropriate as a Rule 12(b) motion to dismiss." *Slyce Acquisition Inc. v. Syte – Visual Conception Ltd.*, No. W-19-CV-00257-ADA, 2020 U.S. Dist. LEXIS 9451, at *11 (W.D. Tex. Jan. 10, 2020). This is because the Federal Circuit has instructed district courts that "[d]etermining patent eligibility requires a full understanding of the basic character of the claimed subject matter." *MyMail, Ltd. v. ooVoo, LLC*, 934 F.3d 1373, 1379 (Fed. Cir. 2019). Claim construction can affect "and perhaps, in most cases, will affect" the Section 101 eligibility analysis—this case being no exception—so courts take the view that "it is generally wiser-and more efficient-to wait to determine a patent's § 101 eligibility until after issuing [a] claim construction order." *Slyce Acquisition*, 2020 U.S. Dist. LEXIS 9451, at *16; *see also Bancorp Servs., L.L.C. v. Sun Life Assur. Co. of Can.*, 687 F.3d 1266, 1273-74 (Fed. Cir. 2012) ("[I]t will

ordinarily be desirable—and often necessary—to resolve claim construction disputes prior to a § 101 analysis."').¹¹ Indeed, the parties here appear to have drastically different opinions about the focus of the claims of the '705 Patent. The Court will be in a better position to address these issues after claim construction, when it has a more complete understanding of the basic character of the claimed subject matter.¹²

E. Claim 19 Is Not Representative Of All Claims

The Motion should also be denied as to all claims except claim 19 because claim 19 is not representative of all remaining claims. Indeed, various other claims recite additional concrete details of *how* the proposed abstract idea is implemented that require different considerations. For example, claim 4 describes a specific way of detecting an insecure condition that is not addressed by Citrix's analysis of claim 19: configuring an operating system to quarantine the first host upon initial startup. Claim 14 includes similar subject matter. Although Citrix attempts to dismiss these as merely related to the detection of an insecure condition, precedent is clear that specific ways of implementing even abstract ideas may be patentable. *See Amdocs*, 841 F.3d at 1312 ("[O]nly claims specifying *how* to overcome those technological challenges are eligible."). As another example, claims 5 and 6 likewise provide specific details for *how* the first host is permitted to communicate with the remediation host despite the quarantine. Contrary to Citrix's contentions, these are not mere "conditions" on the independent claims. (Motion at 7.)

¹¹ Although K.Mizra acknowledges this Court is bound by current Federal Circuit precedent on whether Section 101 issues may be decided at this stage, at least one Federal Circuit judge has suggested the Federal Circuit should reconsider that precedent. *Nat. Alternatives Int'l, Inc. v. Creative Compounds, LLC*, 918 F.3d 1338, 1354 (Fed. Cir. 2019) (Reyna, dissenting-in-part) ("This case, and the general development of the law concerning § 101 analysis at the pleading stage, causes me to ask whether the time has come for this court to reconsider whether a Rule 12(c) motion based on § 101 should be decided before claim construction.").

¹² For example, the Court's construction of the terms "trusted computing base" and "trusting computing module" will likely be useful to the Court in determining whether use of these systems in the claimed context is conventional, as Citrix alleges. (Motion at 17.) Citrix's Reply may raise potential construction issues with other terms, such as "insecure condition" (to the extent that Citrix insists this term is somehow comparable to being unvaccinated), "protected network" (to the extent that Citrix insists this term is somehow comparable to a public school), "valid digitally signed attestation of cleanliness" (to the extent that Citrix insists this is somehow comparable to proof of vaccination), and perhaps others. However, because Citrix failed to meaningfully address the claim language, K.Mizra is unable to identify every term whose construction may impact the outcome of the subject matter eligibility issue.

IV. CONCLUSION

The Court should deny Citrix's Motion. However, if the Court is inclined to grant the Motion on the present record, K.Mizra respectfully requests an opportunity to amend the Complaint to provide a more complete description of the issues relevant to the Motion. *See Aatrix I*, 882 F.3d at 1128 (finding abuse of discretion to deny leave to amend where amendment could provide additional factual allegations to support patentability).

Dated: June 24, 2025

Respectfully Submitted,

/s/ Gerald E. Greenberg

GERALD E. GREENBERG

Florida Bar No. 440094

ggreenberg@gsgpa.com

ALESSANDRA M. SIBLESZ

Florida Bar No. 1024843

asiblesz@gsgpa.com

GELBER SCHACHTER & GREENBERG, P.A.

One Southeast Third Avenue, Suite 2600

Miami, Florida 33131

Telephone: (305) 728-0950

E-service: efilings@gsgpa.com

ROBERT R. BRUNELLI*

CO State Bar No. 20070

rbrunelli@sheridanross.com

BRIAN S. BOERMAN*

CO State Bar No. 50834

bboerman@sheridanross.com

SHERIDAN ROSS P.C.

1560 Broadway, Suite 1200

Denver, CO 80202

Telephone: 303-863-9700

**Admitted pro hac vice*

Counsel for Plaintiff K.Mizra LLC